Amazon Virtual Private Cloud (VPC)

- Networking Layer of EC2
- Logically Isolated Virtual Network
  - Can span multiple AZs
  - Largest IP address range /16
  - Traffic monitored with VPC Flow Logs
- 1 Default VPC Per Account Per Region
  - 5 VPCs Per Account Per Region
- Key Components
  - Subnets
    - Container for AWS resources
    - Segment of IP range in a VPC
      - Defined by CIDR blocks
        - Smallest subnet contains 16 IP address with /28
        - AWS reserves first 4 and last 1 IP addresses
    - 1 or more subnets in each AZ
      - 1 default subnet created for each AZ in default VPC
      - 1 subnet to 1 AZ - cannot span AZ
      - 200 subnets per VPC
    - Public
      - Route table directs traffic to IGW
    - Private
      - Route table does not direct traffic to IGW
    - VPN-only
      - Route table directs traffic to VPG and no route to IGW
  - Route Tables
    - Allow EC2 instances from different subnets within a VPC to communicate with each other
    - Each subnet must be associated with a route table
    - Each VPC has an implicit router
      - Comes w/ a main modifiable route table
    - Custom route tables can be added
    - Contains a non-modifiable and non-removable local route to enable communications within a VPC
    - Routes determine if associated subnet is public, private, or VPN-only
  - Dynamic Host Configuration Protocol (DHCP) Option Sets
    - Default DHCP option set automatically created for a VPC
      - Each VPC can only have 1 DHCP option set assigned
    - Can create custom DHCP option set
      - Allow assign your own domain name to instances
      - Up to 4 domain name servers
      - domain-name
      - ntp-servers
      - netbios-name-servers
      - netbios-node-type set to 2
  - Security Group

    - Required for EC2 instances
    - Virtual stateful firewall at instance level
    - Default security group
      - Allows all instances associated to communicate with each other
      - Allows all outbound traffic
      - Denies all other traffic
      - Can be modified but cannot be deleted
    - Custom security group
      - Instances associated with the same security group cannot talk to each other by default
      - Allow all outbound traffic by default
      - Allow no inbound traffic by default
      - Can only specify allow rules, not deny rules
      - Separate rules for inbound and outbound traffic
    - Changes to security group take effect immediately
    - Evaluate all rules before deciding to allow traffic
    - Limits
      - Up to 500 security groups can be created per VPC
      - Up to 50 inbound and 50 outbound rules per security group
      - Up to 5 security groups can be associated with each network interface
  - Network Access Control Lists (ACLs)
    - A layer of security at subnet level
    - A stateless firewall on a subnet level
    - VPC created with a modifiable default ACL
      - Default ACL is associated with every subnet
        - Allows all inbound and outbound traffic
    - Custom ACL can be created
      - Denies all inbound and outbound traffic by default
    - Process rules in increasing number order when deciding to allow traffic
- Optional Components
  - Internet Gateways (IGW)
    - Allows traffic between instances and internet
    - Horizontally scaled, HA
      - Fully redundant with no bandwidth constraints
    - 1 IGW per VPC
    - A target in route table
    - Network address translation for instances with public IP
    - Used to create public subnet
      - Attach IGW to a VPC
      - Create a subnet route table rule to send non-local traffic to IGW
      - Configure network ACLs and security group rules
  - Elastic IP Addresses (EIPs)
    - Static, public IP address
    - Allocated from a pool for a region
      - Assigned to an instance

    - Can be moved from one instance to another within the same region
    - 5 EIP addresses per account per region
  - 1-1 relationship with network interface
  - Remain associated with an account until explicitly released
  - Charges apply to EIP even if it is not associated with a resource
- Elastic Network Interface (EINs)
  - Virtual network interface
  - Can be attached to an instance within the same AZ and the same VPC
    - Allow instance network presence in different subnets
  - Associated with a subnet upon creation
  - Can have 1 public IP and multiple private IPs
  - Persists regardless the lifetime of instance
- VPC Endpoints
  - Enable private connections between VPC and another AWS service
    - Only supports S3 service currently
    - No need to access internet
    - No need to go through NAT instance
    - No need for VPN
    - No need for AWS Direct Connect
  - Can create multiple endpoints for a single service
  - Can configure multiple route tables
    - Use different route tables to enforce different policies from different subnets
- Peering
  - Networking connections between two VPCs
    - Can be within the same account
    - Can be in different accounts within the same region
    - Same bandwidth as if they are in the same VPC
    - Peered VPCs must have non-overlapping IP ranges
  - Not a gateway or VPN connection
  - No single point of failure
  - Created using request/accept protocol
  - Each VPC can have multiple peering connections
  - Can only have 1 peering agreement between 2 VPCs
  - No transitive routing
- Network Address Translation (NAT) Instances
  - Allow traffic from instances within a private subnet to reach internet
  - Customer-managed instance
  - Should be in a public subnet
  - Must be behind a security group
  - Forward traffic to IGW
  - Configure route table to direct internet-bound traffic to NAT instance
  - Disable source/destination check attribute
  - Allocate an EIP and associate with the NAT instance
- NAT Gateways
  - Allow traffic from instances within a private subnet to reach internet

  - Better availability and higher bandwidth than NAT instance
  - AWS managed service
  - Should be in a public subnet
  - Forward traffic to IGW
  - Configure route table to direct internet-bound traffic to NAT gateway
  - Allocate an EIP and associate with the NAT gateway
  - Recommend to use in production
- Connecting On-prem with VPC
  - Virtual Private Gateways (VPGs and VGWs)
    - AWS end of VPN tunnel
    - Supports dynamic routing with BGP
    - Support static routing
    - 5 VPGs per account per region
    - 10 IPsec VPN Connections per VPG (VGW)
  - Customer Gateways (CGWs)
    - Customer's side of VPN tunnel
    - Hardware or software application
    - 50 customer gateways per account per region
  - Virtual Private Networks (VPNs) tunnel
    - Must initiate from CGW to VPG (VGW)
    - Consists of two tunnels for HA to VPC